EXHIBIT 4

Search Warrant and Application

UNITED STATES DISTRICT COURT

for the

District of Utah

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE RESIDENCE, VEHICLES AND A PERSON LOCATED AT 2929 SOUTH 6500 WEST CEDAR CITY, UTAH 84720

Case No. 4:21-mj-00074-PK

Filed Under Seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A.

located in the _____ District of Utah , there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1958(a)	Use of Interstate Commerce Facilities in the Commission of Murder-For-Hire

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Brian M. DeCarr, FBI Special Agent
Printed name and title

Attested to by the affiant in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Date: 25 Oct. 2021

Judge's signature

City and state: St. George, Utah

U.S. Magistrate Judge Paul Kohler
Printed name and title

ANDREA T. MARTINEZ, Acting United States Attorney (9313)
STEPHEN P. DENT, Assistant United States Attorney (17405)
Attorneys for the United States of America
20 North Main Street, Suite 208
St. George, Utah 84770
Telephone: (435) 634-4262
stephen.dent@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A WARRANT TO SEARCH THE RESIDENCE LOCATED AT 2929 SOUTH 6500 WEST IN CEDAR CITY, UTAH	**FILED UNDER SEAL** **AFFIDAVIT** Case No. 4:21-mj-00074-PK Magistrate Judge Paul Kohler

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Brian M. DeCarr, being duly sworn, depose and state that:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed since January 2020. I am currently assigned to the Albany, New York Field Office. My current duty assignment is with the Capital District Safe Streets Task Force in Albany. In that assignment, I work with federal, state, and local law enforcement agents and officers in investigating criminal activities such as violent crime and transnational organized crime. Prior to my employment with the FBI, I was a New York State Trooper from May 2018 until January 2020, and was a Police Officer for the Pentagon Force Protection Agency from June 2017 until May 2018. I have participated in the execution of numerous warrants involving the search and seizure

of financial records, computers, computer equipment, software, and electronically stored information.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7) — that is, an officer of the United States who is empowered by law to conduct investigations of offenses enumerated in Title 18, United States Code, Section 2516(1). Accordingly, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including offenses related to Title 18 U.S.C. § 1958(a) (Use of Interstate Commerce Facilities in the Commission of Murder-For-Hire), which statute provides in pertinent part that:

> "Whoever… uses… any facility of interstate or foreign commerce, with intent that a murder be committed in violation of the laws of any State or the United States as consideration for the receipt of… anything of pecuniary value [is guilty of a crime]."

3. I submit this affidavit in support of a search warrant application, made pursuant to Federal Rule of Criminal Procedure 41, to search the property located at 2929 South 6500 West in Cedar City, Utah), as further described in Attachment A (the "SUBJECT PREMISES"), for evidence of violations of 18 U.S.C. § 1958(a) (Use of Interstate Commerce Facilities in the Commission of Murder-For-Hire) (as further described in Attachment B). Both Attachments A and B are incorporated herein by reference.

4. I make this affidavit from personal knowledge based on my participation in this investigation, including victim interviews, witness interviews and review of reports by myself and/or other law enforcement agents, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.

5. The information outlined below is provided for the limited purpose of establishing probable cause for a search warrant to search the SUBJECT PREMISES described in Attachment A for the items described in Attachment B, and does not contain all details or all facts known to me regarding this investigation.

PROBABLE CAUSE

Background

6. On September 2, 2021, the FBI Albany Field Office received information from the FBI Knoxville Field Office regarding information received from a confidential source that included communications purportedly retrieved from a Darknet website accessible via The Onion Router (TOR) network depicting a user of the website paying Bitcoin in exchange for the killing of two individuals who reside in Hoosick Falls, New York for an agreed upon amount of approximately $16,000 United States currency.

Confidential Source

7. The FBI confidential source, who is cooperating voluntarily and has received payments solely to offset incurred costs, has previously provided records of communications and payments received from an individual with access to the Darknet website, which subsequent FBI investigations confirmed depicted actual attempts to hire "hitmen" to kill real individuals using the same Darknet website. Specifically, in those approximately 40 investigations, the FBI was able to identify the users who placed the orders and made the payments, and confirmed through forensic evidence and admissions by the users involved that the records of communications and payments were authentic and accurate.

Content of Communications over the Darknet Website

8. In this case, the communications, which occurred between July 16 and August 9, 2021, depict an anonymous user interacting on the Darknet website with another user and a site administrator to arrange the killing of the two above-referenced individuals in exchange for what was approximately $16,000 worth of the cryptocurrency Bitcoin. The anonymous user provided the site administrator with the names, address and photographs of the intended victims, as well as the manner in which the killing should take place. Specifically, the user advised that the killing should be made to look like an accident or botched robbery, and that, if possible, care should be taken to not harm any of the three children known to be in the case of the intended victims.

9. In the course of the Darknet website communications, the anonymous user is depicted transferring the requested approximately $16,000 worth of Bitcoin in a series of payments to the site administrator using various means, including the cryptocurrency wallet service Samourai, which advertises itself as means for shielding cryptocurrency transfers from financial surveillance of the cryptocurrency's blockchain. At this time, it is believed that the Darknet website is in fact a scam operation, and that after payment is delivered to the website no one is dispatched to carry out killings. This belief is premised on information provided by the confidential source, and the fact the prior investigations did not reveal any actual "hitmen" having been dispatched to kill the intended victims in those cases.

The Bitcoin Transactions

10. The Bitcoin transactions depicted in the Darknet website communications provided certain information regarding the aforementioned wallet and other cryptocurrency exchanges being used for the transaction, such that the FBI National Cyber Investigative Joint Task Force (NCIJTF), was able to identify the cryptocurrency exchanges used to make the Bitcoin payments

to the Samourai wallet, which was used to make the payments to the Darknet website based on certain identifiers associated with the transactions.

11. An exigent request for information associated with the account was submitted to one of the cryptocurrency exchanges, Coinbase, which complied with the request, as well as a subsequent grand jury subpoena, and was able to provide subscriber information for the account user, as well as a detailed record of the funds transferred in and out of the account and IP logins associated with the user's transactions.

Cryptocurrency Account Information

12. The subscriber information in the cryptocurrency exchange account identified CHRISTOPHER PENCE as the account holder (including his date of birth and social security number), along with additional user-provided information, including the address 2929 South 6500 West Cedar City, Utah 94720 (i.e. the SUBJECT PREMISES), the email address ap.cpence@gmail.com, the phone number (425) 220-4014, a linked bank account at the Boeing Employee Federal Union (BECU), and a Utah driver's license number. PENCE's identity was verified by the cryptocurrency exchange via a valid driver's license which included a photograph of PENCE, which the FBI additionally corroborated.

Analysis of IP Logins

13. Analysis of the IP addresses associated with the transactions conducted by the user of the Coinbase account revealed that the IP address assigned to the user of the account for 66 out of the 67 transactions that logged the user's IP address was 70.34.15.207, which is an IP address assigned by the internet service provider InfoWest (headquartered at 435 East Tabernacle Street St. George, UT 84770). These logged transactions included three of the transactions that corresponded with the dates, times and amounts that deposited Bitcoin into the wallet that send the

payments to the Darknet website. Responsive records received from InfoWest in response to a grand jury subpoena revealed that the above IP addresses is static, and have been exclusively assigned to an account with PENCE as the subscriber and the SUBJECT PREMISES as the location of the service. The service has been provided to the SUBJECT PREMISES since November 2020, and is currently in effect.

14. The only other IP addresses associated with a logged transaction according to the cryptocurrency exchange's records – which happened to be a Bitcoin deposit – was an IP address that was assigned by Verizon Wireless. Responsive records received from Verizon Wireless in response to a grand jury subpoena revealed that the IP address in question was, and currently remains, assigned to an account – phone number (425) 220-4014 – whose subscriber is PENCE with the SUBJECT PREMISES as the subscriber's residential address.

Information Provided by Intended Victims

15. On September 3, 2021, your affiant interviewed the intended victims. The interviews corroborated the information received from the confidential source and from the investigative work done by FBI to the extent that the intended victims matched the descriptions and photographs provided by the anonymous Darknet user, had the same number of children, and resided at the location described.

16. Additionally, the interviews revealed a motive for PENCE, specifically that, among other things, PENCE's family had legally adopted five of the intended victims' children, and that there was an escalating dispute between the two families such that the intended victims desired to regain custody of their children and were involved in the reporting of PENCE's family to local child welfare authorities, both of which reportedly angered PENCE. Furthermore, PENCE and

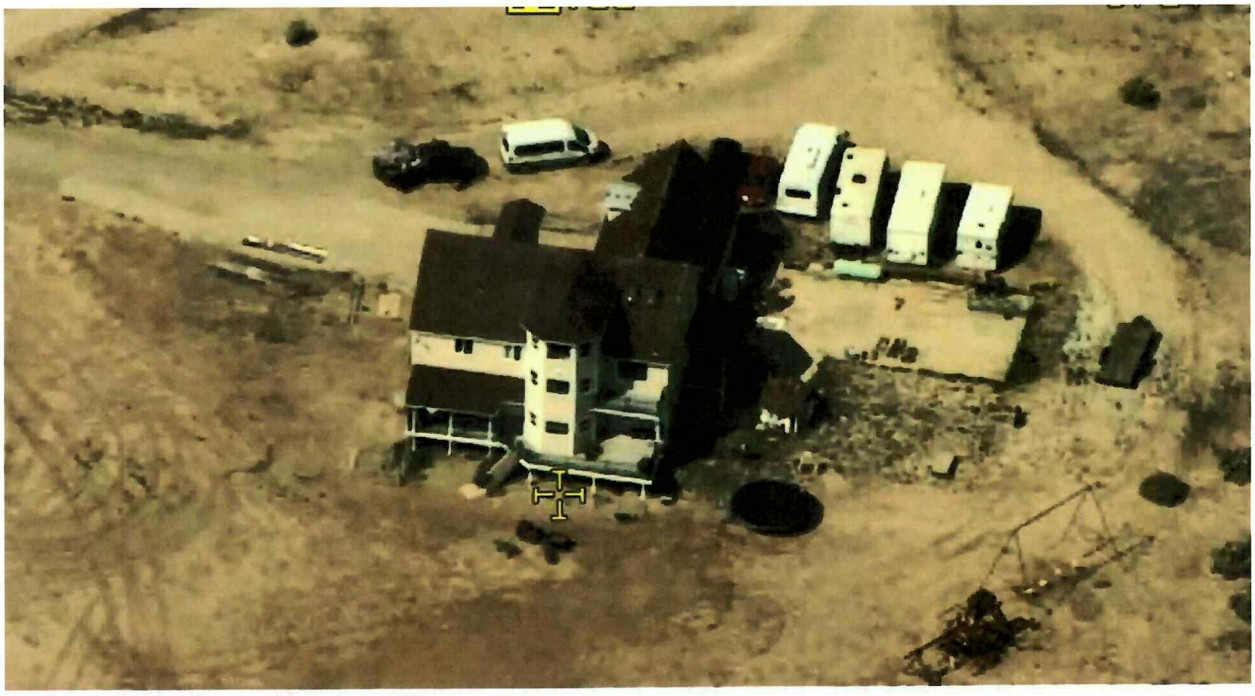
the intended victims did not agree on how the children should be raised or the personal choices and lifestyle of the intended victims.

17. Furthermore, the intended victims recognized the photographs that the anonymous user of the Darknet provided to the Darknet website as part of the placement of the order for the killing of the intended victims, in that the photographs were reportedly the same as those provided by the intended victims to PENCE and his family for use as a "baby book," with the intended victims' children, who were adopted by PENCE.

18. Your affiant further learned that PENCE used the above-referenced Gmail account to communicate with the intended victims, and that all parties communicated via the Google Duo mobile video application.

Surveillance of the SUBJECT PREMISES

19. On September 22, 2021, FBI investigators used a fixed-wing aircraft to surveil the SUBJECT PREMISES, and determined that it appeared to be inhabited based on the presence of multiple individuals present at the location, as well as the existence of a number of vehicles and recreational vehicles, as depicted in the photographs below:



20. Regarding the vehicles, a recent follow-up conversation with one of the intended victims revealed that PENCE and his family frequently used recreational vehicles for family travel, and that PENCE and his family communicated with the intended victims and their family using Internet-capable electronic devices during those trips.

Background Regarding the Internet and Electronic Devices Generally

21. The Internet is a worldwide computer network that connects computers, and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISPs employ dynamic IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses may also be static, if an ISP assigns a user's computer a particular IP address that is used each time that computer accesses the Internet. The ISP may log the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

22. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, e.g., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically

stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Additionally, a computer also creates logs, indices, and registries indicating when a computer was used, which user was logged on, and when data was accessed, shared, transferred, or downloaded. A forensic examiner can often recover evidence that shows that a computer contains peer-to-peer software (see below), when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data. Cellular telephones also allow the user to save or store text messages and email messages received by the phone, for later viewing or distributing, and even if deleted, a forensic examiner can often recover evidence of such text messages and email messages.

23. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an

electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

Seizing and Searching Computer and Electronic Devices

24. I have spoken with law enforcement personnel trained in computer evidence recovery who have knowledge about the operation of computer systems and the correct procedures for the seizure and analysis of computer systems. These individuals have participated in the execution of numerous search warrants during which they have seized and/or examined computer systems. These individuals have also participated in several warrants that involved the search and/or seizure of computer systems, and have been responsible for analyzing seized electronic data and records from those systems.

25. Based on my experience and training, plus the common-sense knowledge that in today's technological world computers and computer-related media are used for communication and storage of data and information, it is reasonable to believe that some or all of the records sought to be seized will be in electronic/digital format.

26. Furthermore, based upon my training, experience, and consultations with law enforcement personnel who specialize in searching computer systems, I have learned that searching and seizing information from computer systems and other storage media (including PDAs, cell phones, MP3 Players, etc.) often requires agents to seize most or all the computer system or storage media to be searched later by a qualified computer forensic examiner in a laboratory or other controlled environment. This is true for the reasons set out below.

27. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. The hard drives commonly included in mere desktop computers

are capable of storing millions of pages of text; the storage capacity of other electronic devices (e.g. a micro drive, a thumb drive, etc.) can also be significant. Unlike the search of documentary files, computers store data in "files" that cannot easily be reviewed. For instance, a single 1 gigabyte of storage media is the electronic equivalent of approximately 500,000 pages of double spaced text. Most computer and electronic devices have capacities well in excess of a single gigabyte.

28. The search through the computer (or other electronic media) itself is a time-consuming process. Software and individual files can be "password-protected." Files can be placed in hidden directories; files can be mislabeled or be labeled with names that are misleading. Similarly, files that contain innocent appearing names ("Smith.ltr") can in fact be electronic commands to electronically cause the data to self-destruct. Also, files can be "deleted," but, unlike documents that are destroyed, the information and data from "deleted" electronic files usually remains on the storage device until it is "overwritten" by the computer. For example, the computer's hard drive stores information in a series of "sectors," each of which contains a limited number of electronic bytes, usually 512. These sectors are generally grouped to form clusters. There are thousands or millions of such clusters on a hard drive. A file's clusters might be scattered throughout the drive (for example, part of a memo could be at Cluster 163, while the next part of the memo might be stored at Cluster 2053). For a non-deleted file, there are "pointers" that guide the computer in piecing the clusters together. For a file that has been deleted, the "pointers" have been removed. Therefore, the forensic examination would include the piecing together of the associated clusters that made up the "deleted" file. Being aware of these pitfalls, the investigator/analyst must follow a potentially time-consuming procedure to review the contents of

the computer storage device so as to insure the integrity of the data and/or evidence. A single computer and related equipment could take many days to analyze properly.

29. Therefore, based upon my knowledge, training, and experience, as well as information related to me by Special Agents and others involved in forensic examination of computers, I am aware that searches for and seizures of evidence from computers commonly require Agents to seize most or all of a computer system's input/output and peripheral devices (including other storage media), in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. In order to fully retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units ("CPUs"), and applicable keyboards and monitors which are an integral part of the processing unit.

30. Furthermore, searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

31. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover hidden, mislabeled, deceptively named, erased, compressed, encrypted, or password protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

32. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

33. Based upon my training and experience and conversations with other law enforcement personnel, I am aware that a number of computer storage devices are quite small and portable, and can be easily hidden on a person. For instance, smartphones can store numerous digital images on an SD card approximately the size of a postage stamp. In addition, thumb drives, which are approximately the size of a pocket knife, can hold numerous images and computer videos. I therefore also request permission to search the person of CHRISTOPHER PENCE for such evidence.

Biometric Unlocking

34. The warrant I am applying for would permit law enforcement to compel certain individuals to unlock a device subject to seizure pursuant to this warrant using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's

face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device

has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by

law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

i. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face to those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

Search Methodology to be Used

35. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;

b. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. surveying various file directories and the individual files they contain;

e. opening files in order to determine their contents;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

36. Therefore, based upon my experience, training, and the totality of circumstances in the above information, your affiant submits that there is probable cause to believe that PENCE, and possibly other users of the Internet at the SUBJECT PREMISES, are involved in arranging the killing of the intended victims in Hoosick Falls, New York through the use of the Internet and

by providing something of pecuniary value (i.e. approximately $16,000 in Bitcoin), in violation of 18 U.S.C. § 1958(a) (Use of Interstate Commerce Facilities in the Commission of Murder-For-Hire). Additionally, there is probable cause to believe that evidence of the above criminal offense(s) is located in the SUBJECT PREMISES, on the person of PENCE, and within electronic media recovered therefrom, and this evidence, more fully described in Attachment B to this affidavit, which is incorporated herein by reference, is also contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

37. I respectfully request that the proposed warrant be issued authorizing the search of: (A) the residence located at 2929 South 6500 West in Cedar City, Utah (the "SUBJECT PREMISES"), to include any outbuildings on the property under the dominion and control of the resident or occupant of the SUBJECT PREMISES; (B) the person of CHRISTOPHER PENCE; (C) any vehicles located on the SUBJECT PREMISES; and (D) any computers, computer equipment, cellular telephones and/or any other electronic media located during the execution of the search warrant. Located within the places and items to be searched, I seek to seize evidence, fruits, and instrumentalities of criminal violations of 18 U.S.C. § 1958(a) (Use of Interstate Commerce Facilities in the Commission of Murder-For-Hire), as more particularly described in Attachment B.

Attested to by the affiant,

Brian M. DeCarr
Special Agent
Federal Bureau of Investigation

I, the Honorable Paul Kohler, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on October 25, 2021, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure:

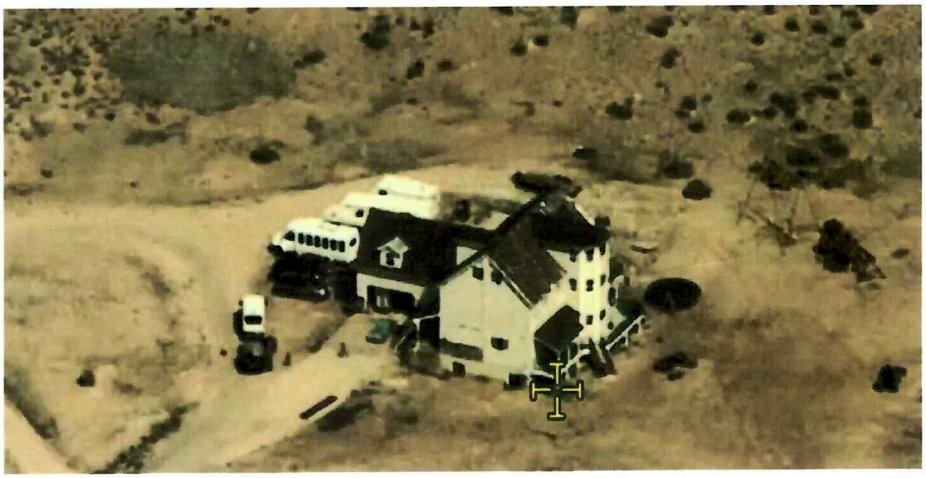
Hon. Paul Kohler
United States Magistrate Judge

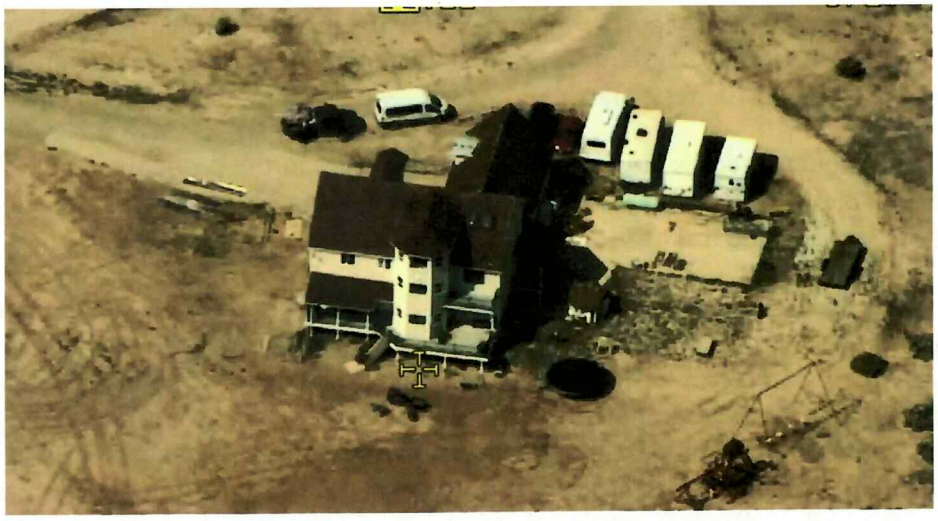
ATTACHMENT A

Places and Items to Be Searched

The places and items to be searched are: 2929 South 6500 West in Cedar City, Utah (the "SUBJECT PREMISES"), to include any outbuildings on the 20-acre property under the dominion and control of the residents or occupants of the SUBJECT PREMISES; (B) the person of CHRISTOPHER PENCE; (C) any vehicles located on the SUBJECT PREMISES; and (D) any computers, computer equipment, cellular telephones and/or any other electronic media located during the execution of the search warrant.

The SUBJECT PREMISES is a tan-colored, three-story, single family, 7-bedroom, approximately 5,800 square foot house situated on a 20-acre lot approximately 500 feet east of South 6500 West, accessed by a gravel driveway leading from South 6500 West in Cedar City, Utah, depicted below:





ATTACHMENT B

Items to be Seized and Searched

Items evidencing violations of Title 18 U.S.C. § 1958(a) (Use of Interstate Commerce Facilities in the Commission of Murder-For-Hire) involving CHRISTOPHER PENCE, including:

Materials Relating to an Online Murder-for-Hire Scheme

1. Records of a resident of the SUBJECT PREMISES using an Internet-capable electronic device to access the Darknet via the via The Onion Router (TOR) network for the purpose of arranging the killing of individuals in Hoosick Falls, New York.

2. Records of the purchase and transferring of cryptocurrency associated with payments made in exchange for the killing of individuals in Hoosick Falls, New York.

3. Records of communications with the intended victims.

4. A book containing the photographs of the intended victims.

5. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, notes, and reference materials.

6. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

7. Records of address or identifying information for the target(s) of the investigation, and any user names, user IDs, eIDs (electronic ID numbers), and passwords.

8. Documents and records, including, for example, receipts, banking records, bills, statements, telephone records, and other similar indicia of ownership indicating occupation, possession, or control over the residence and/or possession of the searched items located therein.

9. Computer records and evidence identifying who the particular user of the Internet at the SUBEJCT PREMISES who arranged payments for the killing of individuals in Hoosick Falls, New York through the use of the Internet (i.e. evidence of attribution).

10. Records of computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

Computers and Electronic Media

11. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other storage media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies), to include (i) records stored in deleted data, remnant data and slack space, (ii) any software capable of interpreting or storing such records, and (iii) any computer-related documentation explaining or illustrating the configuration of any seized computer hardware, software, or related items.

12. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

13. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

14. This warrant authorizes the seizure of electronic storage media and the seizure and copying of electronically stored information for later offsite review consistent with the warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Photographs of Search

15. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

Biometric Unlocking

16. During the execution of the search of the SUBJECT PREMISES, law enforcement personnel are authorized to: (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the
District of Utah

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE RESIDENCE, VEHICLES AND A PERSON LOCATED AT 2929 SOUTH 6500 West CEDAR CITY, UTAH 84720

Case No. 4:21-mj-00074-PK

Filed Under Seal

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer, including members of the New York State Police.

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Utah
(identify the person or describe the property to be searched and give its location):
See Attachment A.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before November 8, 2021
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Paul Kohler .
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30).*
☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 25 Oct. 2021; 3:08 pm

Judge's signature

City and state: St. George, Utah

Paul Kohler, U.S. Magistrate Judge
Printed name and title

Return		
Case No.:	*Date and time warrant executed:*	*Copy of warrant and inventory left with:*
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Places and Items to Be Searched

The places and items to be searched are: 2929 South 6500 West in Cedar City, Utah (the "SUBJECT PREMISES"), to include any outbuildings on the 20-acre property under the dominion and control of the residents or occupants of the SUBJECT PREMISES; (B) the person of CHRISTOPHER PENCE; (C) any vehicles located on the SUBJECT PREMISES; and (D) any computers, computer equipment, cellular telephones and/or any other electronic media located during the execution of the search warrant.

The SUBJECT PREMISES is a tan-colored, three-story, single family, 7-bedroom, approximately 5,800 square foot house situated on a 20-acre lot approximately 500 feet east of South 6500 West, accessed by a gravel driveway leading from South 6500 West in Cedar City, Utah, depicted below:

ATTACHMENT B

Items to be Seized and Searched

Items evidencing violations of Title 18 U.S.C. § 1958(a) (Use of Interstate Commerce Facilities in the Commission of Murder-For-Hire) involving CHRISTOPHER PENCE, including:

Materials Relating to an Online Murder-for-Hire Scheme

1. Records of a resident of the SUBJECT PREMISES using an Internet-capable electronic device to access the Darknet via the via The Onion Router (TOR) network for the purpose of arranging the killing of individuals in Hoosick Falls, New York.

2. Records of the purchase and transferring of cryptocurrency associated with payments made in exchange for the killing of individuals in Hoosick Falls, New York.

3. Records of communications with the intended victims.

4. A book containing the photographs of the intended victims.

5. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, notes, and reference materials.

6. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

7. Records of address or identifying information for the target(s) of the investigation, and any user names, user IDs, eIDs (electronic ID numbers), and passwords.

8. Documents and records, including, for example, receipts, banking records, bills, statements, telephone records, and other similar indicia of ownership indicating occupation, possession, or control over the residence and/or possession of the searched items located therein.

9. Computer records and evidence identifying who the particular user of the Internet at the SUBEJCT PREMISES who arranged payments for the killing of individuals in Hoosick Falls, New York through the use of the Internet (i.e. evidence of attribution).

10. Records of computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

Computers and Electronic Media

11. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other storage media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies), to include (i) records stored in deleted data, remnant data and slack space, (ii) any software capable of interpreting or storing such records, and (iii) any computer-related documentation explaining or illustrating the configuration of any seized computer hardware, software, or related items.

12. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

13. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

14. This warrant authorizes the seizure of electronic storage media and the seizure and copying of electronically stored information for later offsite review consistent with the warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Photographs of Search

15. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

Biometric Unlocking

16. During the execution of the search of the SUBJECT PREMISES, law enforcement personnel are authorized to: (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.